Galactic Advisors Security Assessments

Before Diving In, Connect

Go beyond the weather and sports and ask an open-ended question.
Read the situation if personal or business only questions will be acceptable.

1. Weekend Plans or Vacation Planning: I've been looking into a getaway, what are your favorite spots?
2. Visually cued topics like pets/children/grandkids/hobbies are fun favorites too so use a video call when possible.
3. Charity or local community benefit connections
4. How have you been involved in security planning for your company?
5. Vertical related question, for example: How are the current supply chain issues impacting you?

Conversationally Discuss

Instead of reading the following sets of questions, frame each within the conversation as much as possible.

For example, to ease into the list: I know you want to protect the personally identifiable information of those who work for you and your clients, so let's begin by looking at some of the information you handle, access or store.

Pen Test Questions

Organization Name:
Contact Name:
Contact Email:
Contact Phone:

Status: __Prospect

__Client – needs security stack upgrade

__Client – has our current security stack

Initial Call Questions

What type of sensitive information does your team handle, access, or store?
Check all that apply, including employee data as well as client data.

__Yes __No Personal data
__Yes __No Social security numbers
__Yes __No Employment data
__Yes __No Driver's license numbers
__Yes __No Credit card numbers
__Yes __No Banking and/or investment data

__Yes __No Health care information
__Yes __No Medical records or medical history
__Yes __No Intellectual property
__Yes __No Unsure

Do you allow any of the information we just discussed to be e-mailed?
__Not Applicable __Yes __No __Unsure

Do you allow any of the information we just discussed to be stored or transmitted in cloud file-sharing applications like Dropbox, Google Drive, etc.?
__Not Applicable __Yes __No __Unsure

Microsoft 365
The following questions should be asked if the organization uses Microsoft 365.
Do you use Microsoft 365 for email or file storage?
__Yes __No

When you log into your account are you prompted for a code that is sent to your cell phone or shows up on an application on your cell phone?
__Not Applicable __Sometimes __Always __Never

Once logged into Microsoft 365 do you have an 'Admin' application?
It is a little A with a gear next to it. (You may want to have them log in and inspect. You are looking to see if they have Administrative access with the account they use daily.)
__Not Applicable __Yes __No

If they do have administrative access, check to see if they have two factor properly enabled. Verify that their provider has two factor enabled. Check to see if there are any accounts for backup services.

Backups
This section covers questions that should be asked about their backups.
Does your current IT support provide you evidence that they are performing test restores of your data?
__Daily __Weekly __Monthly __Quarterly __Annually __Never __Not Applicable

Education
The following questions should be asked about their current training program.
How often does your team receive simulated phishing training?
__Weekly __Monthly __Quarterly __Annually __Never __Not Applicable

How often does your team receive security training?
__Monthly __Quarterly __Annually __Never __Not Applicable

Insurance

The following questions should be asked about their current insurance policies.

Do you have a cyber liability insurance policy?
__Not Applicable __Yes __No __Unsure

Do you have crime insurance?
__Not Applicable __Yes __No __Unsure

How recently have you evaluated the level of cyber insurance carried by your organization to verify if it is adequate to protect your organization and your clients or patients from financial loss?
__I Don't Know __90 Days __180 Days __1 Year __3 Years

Policies
The following questions should be asked about their current office policies.

Do you have a work from home policy that includes safeguards for client, patient and organization data?
__Not Applicable __Yes __No

Do you have a “clean desk” policy asking employees to not leave sensitive documents lying on their desk when unattended?
__Not Applicable __Yes __No __Unsure

G
What cyber security policies are being used in your office?

__Yes __ No Acceptable Use Policy
__Yes __No Password Policy
__Yes __No Data Confidentiality Policy
__Yes __No Mobile Device Policy
__Yes __No Bring Your Own Device (BYOD) Policy
__Yes __No Incident Response Policy
__Yes __No Backup and Disaster Recovery Plan
__Yes __No Business Continuity Plan
__Yes __No Remote Access Policy

Wrapping Up

If you are able to initiate the scan on the environment at this time, then do so, walking your prospect or client through the process.

Ask if there is anything else they are concerned about in their vertical and offer to research it for them for your next meeting.

Thank your host for discussing their business with you and set a date to go over the results of the assessment.

Relate findings to business impact.
Preparation for the Readout: You should have at least 3 stories

How do you create a good story?

- "This reminds me…"
- Who was involved
- What happened
- Business impact
- Relate to finding

Story example